WEB SECURITY ISSUES: HOW HAS RESEARCH ADDRESSED THE GROWING NUMBER OF THREATS?

Randy Brown

University of Mary Hardin-Baylor
900 College Street
Belton, TX 76513
(254) 295-5403 (W)
(254) 295-4651 (Fax)
Randy.Brown@umhb.edu

ABSTRACT

The Internet has drastically changed how organizations do business. The World Wide Web (WWW or Web) is becoming increasingly important in doing business, selling to customers, managing relationships with vendors and partners, etc. In fact, many organizations have only a Web presence and do not have a physical location. This increase in reliance on the Internet has opened organizations to a plethora of potential threats, giving rise to a broad area of study focusing on security of Web based resources. This study examines some of the many threats to Web Security and investigates how academic research has approached and addressed these threats.

INTRODUCTION

Ever since the invention of the modern computer, computer security has become an increasingly important area of focus for many organizations. The advent of the Internet and World Wide Web (WWW) has added a whole new dimension to computer security, giving rise to the term "Internet Security" (Babb 2004; Macilwain 1994; Millman 2003) or "Web Security" (Mackey 2003). Prior to the Internet, an attacker had to be able to physically access the computer to be able to exploit any vulnerabilities (Barlas, Dubinsky, Osheroff, Verschoor and Williams 2003; Whitman and Mattord 2003; Wilkes 1991). Dial-up access opened computers up to additional threats which did not have to have physical access to the computer. The Internet opened up a whole new world of threats, making computers vulnerable to anyone with Internet access around

the world (Furnell and Warren 1999; Hancock 2000; McClure, Shah and Shah 2003; Nelms 1999).

Internet security started becoming an issue during the late 1970's and early 1980's when the ARPAnet become more open to everyone and the Internet was "born" (Mackey 2003; McClure et al. 2003; Whitman et al. 2003). According to the EBSCO database, the earliest articles dealing with Internet security issues were published in the late 1980's, nearly a decade after the Internet started becoming public (Eisenberg, Gries, Hartmanis, Holcomb, Lynn and Santoro 1989; Lindley 1989; Marshall 1988). Perhaps this delay was due to a lack of exploitation (or knowledge on how to exploit) of vulnerabilities, but this author believes that the delay was due to a lack of being able to detect intrusions rather than an actual lack of security breaches.

In addition, there are many articles in trade and practitioner journals which discuss Internet security issues, but there seems to be a lack in the number of academic journal articles addressing them. Many academic articles have mentioned various Internet security risks, but few studies have actually been performed which focus on these risks. The purpose of this paper, therefore, is to examine academic research in the area of Internet or World Wide Web security. It will examine some of the primary security threats due to the Internet and how researchers have approached these issues. It will include some trend analysis to try to gain an understanding of how the research has progressed through the years, as well as a journal analysis to gain an understanding of which journal(s) are the most likely to address Internet security risks.

LITERATURE REVIEW

In the past two decades, there have been many articles in the area of Internet and Web security, with the earliest appearing in the late 1980's (Marshall 1988; Seeley 1989; Spafford 1989). A recent search of the EBSCO database revealed more than one million articles dealing with the Internet and WWW. Scholarly, or peer-reviewed, journals accounted for about 95% of them (approximately 950,000). Of these articles, however, less than one tenth appear to deal with security issues.

There have been many types of security issues discussed when writing about the Internet. One of the oldest topics discussed in scholarly journals is the virus (Eisenberg et al. 1989; Lindley 1989; Rochlis and Eichin 1989). Viruses are special computer programs which attach themselves to other programs (Mackey 2003; Whitman et al. 2003). This is commonly referred to as "infecting" the computer program. A special type of virus, called a worm has also been a topic for a long time (Marshall 1988; Palca 1989; Spafford 1989). Worms are viruses that do not require human intervention to propagate and are considered "self-propagating" (Butler 2003; Mackey 2003). Another specialized type of virus, referred to as a "Trojan Horse" is not as destructive and usually simply tries to hide its existence from the user by posing as a legitimate application (Mackey 2003; Schneier 1999).

Hackers have been around almost from the beginning of the Internet (Lindley 1989; Wilkes 1991). Hackers attempt to break into computers to steal or corrupt data. Usually, they are not really very destructive (beyond defacing a web site), but can be very annoying. Originally, hackers were spies of thieves, looking for data to steal to either further their organization's cause or to find ways to use the data for making money (illegally). Now, however, more and more hackers are becoming political activists and use their hacking to make political statements or to humiliate their targets (Hancock 1999; Illia 2003; Woo, Kim and Dominick 2004). Related to these political activists are a new set of hackers called "hacker terrorists" (Butler 2002; Nissenbaum 2004) who break into systems to destroy data or disrupt organizations' operations. Another new hacker is the security consultant who hacks systems to find weaknesses. This type of hacking is referred to as "ethical hacking" (Nissenbaum 2004; Palmer 2001; Zonghao and Zonghao 2001). Crackers are often confused with hackers, but they attack specifically through passwords (Seeley 1989). Crackers attempt to break passwords or, more often, product keys on software.

Another popular topic in research articles is that of Spam, which is unsolicited e-mail (Cranor and LaMacchia 1998; Hoyle 2000; Jones 1999). Spam is not destructive in and of itself, but often carries other malicious threats, such as viruses (Hinde 1999; Powell 2003; Simpson 2003). It can also tie up resources (especially e-mail servers and drive space) which can cost the organization money. In addition, the time required for employees to weed through what is legitimate e-mail and what is spam can be quite significant. This is a type of denial of service (DoS), which is the next topic on our list (Pecora, Owen, Marai, Setiad and Chass 2003). Denial of Service (DoS) attacks attempt to overwhelm a server and either cause it to crash or to be so tied up with processing that it essentially stops (Chang 2002; Hovav and D'Arcy 2003; Neumann 2000; Schwartau 1999). These DoS attacks can render entire networks inoperable, costing large amounts of money due to delays in processing. DoS are not destructive attacks, but are very disruptive. A newer version of DoS attacks are distributed DoS (DDoS) which attack a single server from multiple directions via multiple computers (Douligeris and Mitrokotsa 2004; Sung and Xu 2003; Xu and Lee 2003).

A final topic receiving quite a bit of attention in research is that of Internet Security in general (Babb 2004; Bergeron 2000; Millman 2003). These articles typically focus on the need for computer security and tools for dealing with Internet security. There are many other topics which could be addressed, but have not yet been included. These will be addressed in the future.

TRENDS IN INTERNET SECURITY RESEARCH

In order to gain a fuller understanding of where researchers are in relation to the actual issues in Internet security, we need to examine the publication trends of the topics and specific journals. Searching through these abstracts and articles, we gain a feel for the direction Internet security

research has been headed in, as well as some potential gaps between what needs to be researched and what has actually been addressed.

The first area of interest is which publications have featured articles concerning Internet security. This gives us an indication of where we might want to go to find additional information about internet security issues. Several specific databases were selected for inclusion in this search, including: Academic Search Premier, Business Source Premier, and Computer Source. For academic interest (and to reduce scope) only peer-reviewed journals were included. Please note, however, that more than 95% of the articles initially searched were in peer-reviewed journals, so this does not really exclude very many sources. Initial search terms included any of Internet, Web, or WWW. Additional terms were then used to refine the search and included Computer Security, Hack, Crack, Virus, Worm, Trojan, Denial of Service, and Spam. Pseudonyms were included whenever known.

The Internet began in the late 1960's as ARPAnet and started becoming public in the 1970's (McNurlin and Ralph H. Sprague 2002; Turban, McLean and Wetherbe 2001). As Table 1 indicates, however, Internet security articles did not begin showing up until the mid 1980's. This raises questions about why there were so few articles during the first 25 years of the Internet. Perhaps it took several years for intruders to discover how to utilize the Internet. Another possibility is the delay inherent in academic research related to the time it takes to research, document, submit, revise, etc. an article before it actually gets published. The lack of intrusion detection capabilities is another factor which likely affected the number of articles. Whatever the reasons, it has only been during the last ten years that academic interest in Internet security issues has really been piqued. The graph depicted in Figure 1 shows the twenty year trend. The curve indicates an almost exponential growth during these years. Note that there is a significant drop in 2001, but 2002 picks back up on the same curve as if there was no drop in 2001. There are no real indicators for the drop in 2001. Perhaps there was a buildup for "Y2K" issues, then a let down after Y2K. Perhaps there were significant events which led researchers in a different direction. In any case, research in Internet security has resumed growth as if there was not a drop in 2001.

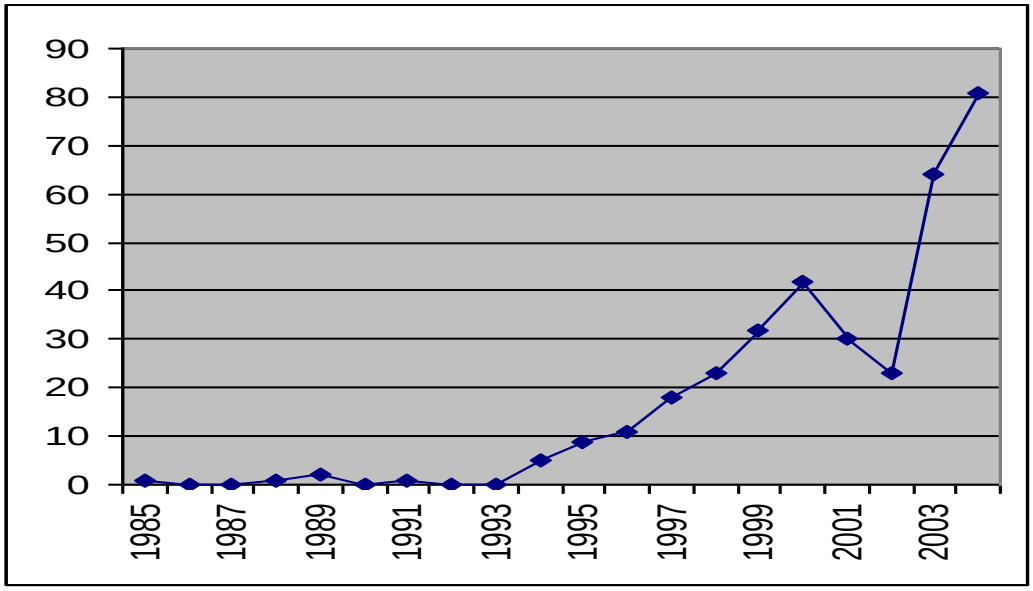

Figure 1: Historical Internet Security Research Trends

There have been quite a few topics investigated by these articles during the last twenty years. Figure 2 represents historical trends for all Internet security issues combined for the last 20 years. As expected, this graph follows closely with the graph in Figure 1 representing only articles and not specific security issues.

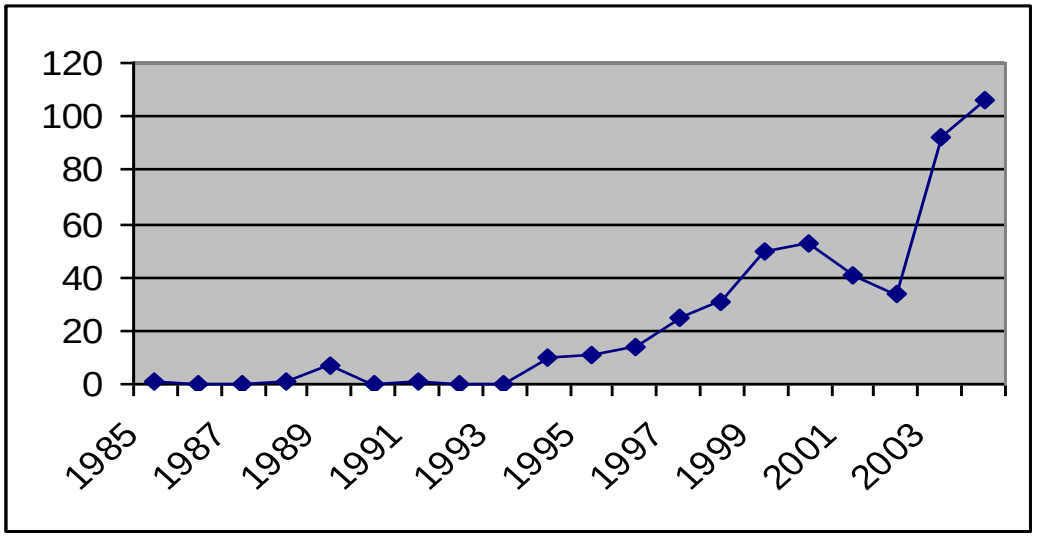

Figure 2: Historical Research Trends for all Internet Security Issues Combined

RESEARCH FRAMEWORK

While there are many articles which mention Internet security issues, there are very few which empirically investigate the issues (Griffiths 2000). In fact, during the course of this survey, only three empirical studies were discovered. The first (Gattiker and Kelley 1999) examines ethical perspectives users have about the use of the Internet and WWW. A second (Kreidl and Frazier 2004) looks at the effectiveness of an automatic worm prevention system. The third (Resnick, Hansen and Richardson 2004) focuses on filtering systems used to prevent access to inappropriate material for specific web users, such as pornography for children.

Research indicates there are several different perspectives which may be used to describe Internet security threats. One of these dimensions is accidental or intentional attacks (Freeman 2000; Nelms 1999; Neuberger and Levetown 2004; Wasserman 1999). Intentional attacks are conscious attempts to destroy data, steal information, disrupt activities, etc. Accidental threats are unconscious activities and come in many forms, such as accidentally deleting a file, e-mailing classified material to an inappropriate person, executing a file containing a virus, etc. These can be very difficult to control and measure.

A second dimension relates to the data or information damage caused by an attack. Many attacks specifically attempt to destroy data and are purely malicious. Others are harmless or just nuisances. Most categories of threats have instances ranging from one extreme to the other, but have certain tendencies. For the purposes of this framework, the threats will be classified according to the general trend of the category to be either destructive or non-destructive.

A third perspective is that of financial impact of Internet security threats. Many attacks may not be destructive or intentional, but they are costly to an organization. Looking only at the two dimensions of destructiveness and intentional, therefore, does not give the entire picture. Measuring financial impact, however, requires much more information than that available during the course of this survey. Therefore, only the two dimensions of destructiveness and intentionality are focused on in this paper.

Figure 3 depicts the two-by-two matrix of the two dimensions and categorizes the Internet security threats into the four quadrants. Many of the threats have aspects which may fit in more than one quadrant. However, there are general trend each threat follows, leading to this particular categorization of the threats. This is only one opinion of how these threats may be categorized and are based on the researcher's understanding of the threats as discussed in the articles reviewed. Obviously, there may be other logical categorization schemes, but this one provides researchers with an excellent starting point.

	More Destructive	Less Destructive
Accidental	Deletion of Data	Send e-mail to wrong person Disclose private info Attach wrong file to e-mail Access inappropriate Websites Time lost surfing Web
Intentional	Virus Worm	Trojan Horse Hacking Cracking Spoofing SpyWare Masquerading ID Theft Piracy DoS Spam

Figure 3: Categorization Framework of Internet Security Threats

Interestingly, most Internet security threats are relatively non-destructive. While the threats on the non-destructive side of the framework are occasionally very destructive, the trends for all of them are not. Trojan horses, while being a type of virus, do not normally exhibit the destructiveness of their cousins. Trojans typically want to remain hidden so they can collect information to send to their creators without the victim becoming aware of them. They are, therefore, usually not destructive, but can be quite costly to organizations by capturing information, such as passwords, and revealing this information to their creators, allowing unauthorized access to proprietary information.

Another major problem is the proliferation of Spam, which has been increasing at an alarming rate. Spam is not destructive in and of itself, but it often carries viruses, SpyWare, Trojan horses, or other malicious software (MalWare) which can be destructive. Spam's greatest threat is due

to the time consumed in weeding through e-mails to determine what is legitimate and what is not. Often, a legitimate e-mail may be deleted accidentally when clearing a system of Spam. Another impact of Spam occurs when an e-mail account or server becomes so overloaded with Spam that legitimate e-mails are rejected or lost. This results in a kind of denial of service (DoS), which is the last in the non-destructive/intentional quadrant of Figure 3. DoS attacks are not destructive (unless the server crashes and loses data as it crashes), but can be very costly due to delays in processing information.

In the accidental, but less destructive quadrant, we have several topics which can cause organizations problems when dealing with Internet activities. Many employees spend a large amount of time on the Internet or dealing with e-mail. These are not data destructive activities, but can be disruptive to operations and could be costly due to lost time or inefficiencies. The other issues in the quadrant deal with information given to the wrong recipients. Sometimes a wrong e-mail address is typed or selected from the address book. Other issues deal with attaching the wrong file or including classified, sensitive, private, etc. material in e-mails either through attachments or in the e-mail body. Again, these activities can be quite costly to an organization, but are not really destructive.

CONCLUSIONS

There are several limitations to this study, but it should still be an excellent starting point for researchers in the area of Internet security, providing an overview of previous literature and a framework for classifying threats. The first limitation is with the database used for locating the articles, which has many resources, but is not all-inclusive. It only contains a few of the thousands of journals available as outlets for publication of Internet security issues. In addition, many of the journals which are included have only limited volumes available for searching, many only containing the last couple of years. This may be one of the reasons for the limited numbers of hits prior to the last ten years. Other journals are scanned and converted to text and contain errors which may prevent effective searching of keywords in those journals.

A second limitation is the manner of the search. Only keywords were used to locate articles. Therefore, the search results are limited by the keywords used. Every effort was used to ensure all appropriate keywords were used for each topic searched; however, it is nearly impossible to include all possible variations. In addition, the term "Internet" only started to become common in the 1980's and the "World Wide Web" only came into being in the 1990's. Therefore, the search may have been limited in years prior to "Internet" and "WWW" becoming commonly used terms.

Another limitation is that only a single researcher performed the search and codification of the articles. In addition, this same author solely classified the security issues in the framework. While the author believes the classifications are appropriate based on prior literature, other

researchers should take caution when applying the framework to ensure they are studying these phenomena appropriately.

Financial impact has been difficult to ascertain, but may actually be the most important dimension for studying WWW security. This is, therefore, an important concept for further research

In conclusion, this study has been a useful exercise for discovering the status of academic research in the area of Internet and WWW security. We have seen that while there are many security issues presented by the proliferation of the Internet and WWW, there has been very little empirical research investigating the phenomena. The framework provides an excellent starting point for classifying the issues and determining which may be more important based upon impact to an organization.

REFERENCES

Babb, M. (2004) Internet Security: Are We Living in the 'Good Ole Days'? *Computing & Control Engineering*, 15, 1, 2

Barlas, S, Dubinsky, J, Osheroff, M, Verschoor, C, and Williams, K. (2003) Protecting Digital Assets, *Strategic Finance*, 85, 6, 3-7

Bergeron, B.P. (2000) It may be fast but is it safe? *Postgraduate Medicine*, 108, 1, 31

Butler, D. (2002) Who's been looking at your data? *Nature*, 418, 6898, 580

Butler, D. (2003) Experts fear network paralysis as computer worms blast Internet, *Nature*, 425, 6953, 3

Chang, R.K.C. (2002) Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial, *IEEE Communications Magazine*, 40, 10, 42

Cranor, L.F, and LaMacchia, B.A. (1998) Spam!, *Communications of the ACM*, 41, 8, 74-83

Douligeris, C, and Mitrokotsa, A. (2004) DDoS attacks and defense mechanisms: classification and state-of-the-art, *Computer Networks*, 44, 5, 643

Eisenberg, T, Gries, D, Hartmanis, J, Holcomb, D, Lynn, M.S, and Santoro, T. (1989) The Cornell Commission On Morris and the Worm, *Communications of the ACM*, 32, 6, 706

Freeman, E.Q. (2000) Identification of Cyber Risks, *Financial Executive*, 16, 3, 32-48

Furnell, S.M, and Warren, M.J. (1999) Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium? *Computers & Security*, 18, 1, 28

Gattiker, U.E, and Kelley, H. (1999) Morality and Computers: Attitudes and Differences in Moral Judgments, *Information Systems Research*, 10, 3, 233

Griffiths, M. (2000) Does Internet and Computer "Addiction" Exist? Some Case Study Evidence, *CyberPsychology & Behavior*, 3, 2, 211-218

Hancock, B. (1999) Hackers Attack US Government Web Sites in Protest of Chinese Embassy Bombing, *Computers & Security*, 18, 4, 279

Hancock, B. (2000) Security Views, *Computers & Security*, 19, 5, 382

Hinde, S. (1999) E-mail Can Seriously Damage Your Health, *Computers & Security*, 18, 5, 396

Hovav, A, and D'Arcy, J. (2003) The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms, *Risk Management & Insurance Review*, 6, 2, 97-121

Hoyle, J. (2000) E-Mail, Hold the Spam, *Journal of the American Dental Association*, 131, 10, 1426

Illia, L. (2003) Passage to cyberactivism: How dynamics of activism change, *Journal of Public Affairs (Henry Stewart)*, 3, 4, 326-337

Jones, F. (1999) Spam: Unsolicited Commercial Email by Any Other Name, *Journal of Internet Law*, 3, 3, 1

Kreidl, O.P, and Frazier, T.M. (2004) Feedback Control Applied to Survivability: A Host-Based Autonomic Defense System, *IEEE Transactions on Reliability*, 53, 1, 148-166

Lindley, D. (1989) Hacker's intentions key to court case, *Nature*, 340, 6232, 329

Macilwain, C. (1994) Spy interests wrecking Internet security, Congress told, *Nature*, 368, 6471, 486

Mackey, D. (2003) Web Security for Network and System Administrators, Course Technology, Boston, MA

Marshall, E. (1988) The worm's aftermath, *Science*, 241, 4882, 1121

McClure, S, Shah, S, and Shah, S. (2003) Web Hacking, Pearson Education, Boston

McNurlin, B.C, and Ralph H. Sprague, J. (2002) Information Systems Management in Practice, Pearson Education, Upper Saddle River, New Jersey

Millman, G.J. (2003) Internet Security: You Don't Get What You Pay For, *Financial Executive*, 19, 9, 51-52

Nelms, C. (1999) Internet E-mail Risks and Concerns, *Computers & Security*, 18, 5, 409

Neuberger, M.J, and Levetown, A.S. (2004) Special Employment Considerations to Ensure the Security of Your IT Department, *Employment Relations Today*, 31, 1, 35-42

Neumann, P.G. (2000) Denial-of-Service Attacks, *Communications of the ACM*, 43, 4, 136

Nissenbaum, H. (2004) Hackers and the contested ontology of cyberspace, *New Media & Society*, 6, 2, 195-217

Palca, J. (1989) Culprit found at Cornell, *Nature*, 338, 6216, 530

Palmer, C.C. (2001) Ethical hacking, *IBM Systems Journal*, 40, 3, 769

Pecora, T.A, Owen, M.C, Marai, C.N.J, Setiad, D.H, and Chass, G.A. (2003) Bridging the gap between pure science and the general public: comparison of the informational exchange for these extremities in scientific awareness, *Journal of Molecular Structure: Theochem*, 666-667, 699

Powell, W. (2003) Scam Is the New Spam, *T+D*, 57, 6, 22

Resnick, P, Hansen, D.L, and Richardson, C. (2004) Calculating Error Rates for Filtering Software, *Communications of the ACM*, 47, 9, 67-71

Rochlis, J.A, and Eichin, M.W. (1989) With Microscope and Tweezers: The Worm from MIT's Perspective, *Communications of the ACM*, 32, 6, 689

Schneier, B. (1999) The Trojan Horse Race, *Communications of the ACM*, 42, 9, 128

Schwartau, W. (1999) Surviving Denial of Service, *Computers & Security*, 18, 2, 124

Seeley, D. (1989) Password Cracking: A Game of Wits, *Communications of the ACM*, 32, 6, 700

Simpson, P. (2003) Spoofed Identities: Virus, Spam or Scam? *Computer Fraud & Security*, 2003, 10, 6

Spafford, E.H. (1989) Crisis and Aftermath, *Communications of the ACM*, 32, 6, 678

Sung, M, and Xu, J. (2003) Ip Traceback-Bases Intellegent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks, *IEEE Transactions on Parallel & Distributed Systems*, 14, 9, 861-872

Turban, E, McLean, E, and Wetherbe, J. (2001) Information Technology for Management, John Wiley & Sons, Inc, New York

Wasserman, D. (1999) Will Insurers be Relevant in the 21st Century? *Risk Management (00355593)*, 46, 4, 14

Whitman, M.E, and Mattord, H.J. (2003) Principles of Information Security, Course Technology,

Wilkes, M.V. (1991) Revisiting Computer Security in the Business World, *Communications of the ACM*, 34, 8, 19-21

Woo, H.-j, Kim, Y, and Dominick, J. (2004) Hackers: Militants or Merry Pranksters? A Content Analysis of Defaced Web Pages, *Media Psychology*, 6, 1, 63-82

Xu, J, and Lee, W. (2003) Sustaining Availability of Web Services under Distributed Denial of Service Attacks, *IEEE Transactions on Computers*, 52, 2, 195

Zonghao, B, and Zonghao, B. (2001) An ethical discussion on the network economy, *Business Ethics: A European Review*, 10, 2, 108

References should follow the APA style. Examples:

Alavi, M. (1994). Computer-Mediated Collaborative Learning: An Empirical Evaluation. *MIS Quarterly 18*(2), 159 - 174

Introna, L. (1997). Management, Information and Power: A narrative of the involved manager. London: MacMillan